Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
	)	

COMMENTS OF TRANSACTION NETWORK SERVICES, INC.

Transaction Network Services, Inc. (TNS), by its attorneys, hereby provides comments in response to the Federal Communications Commission's (FCC or Commission) Third Further Notice of Proposed Rulemaking (hereinafter, 3rd FNPRM)[1] seeking comment on a proposal to accelerate the date by which small voice providers that originate an especially large amount of call traffic must implement the STIR/SHAKEN caller ID authentication framework pursuant the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.[2] TNS supports the Commission's proposal to accelerate the deployment deadline for small voice service providers and offers its views on how best to tailor the rule to those types of providers that are most closely associated with originating problematic calls.

I. ACCELERATION OF THE IMPLEMENTATION DEADLINE FOR SOME PROVIDERS WILL HELP REDUCE ILLEGAL ROBOCALLS

TNS sees the reduction in unwanted and illegal robocalls as a central part of its mission. Two of TNS' leading products, Call Guardian and Call Guardian Authentication Hub, assist voice service providers in managing inbound robocalls and implementing STIR/SHAKEN, respectively. The combination of the use of call analytics and greater implementation of

---

1 *Call Authentication Trust Anchor*, Third Further Notice of Proposed Rulemaking, FCC 21-62, WC Docket No. 17-97 (rel. May 21, 2021) ("3rd FNPRM").

2 Pub. L. No. 116-105, 133 Stat. 3274 (2019).

STIR/SHAKEN is enabling voice service providers to better identify problematic calls and to protect consumers from harm from scam robocalls. Although much work is still to be done, the industry is making significant progress in addressing the problem of illegal and nuisance calls.

As the Commission notes in the *3rd FNPRM*, TNS data shows that problematic robocalls increasingly are shifting to smaller carrier networks.[3] TNS' most recent Robocall Investigation Report shows that 95% of the high risk robocalls originate on non-Tier 1 network resources.[4] This is an increase of 3% from the prior year. As large carriers continue to implement STIR/SHAKEN, and continue to adopt analytics technology to detect and mitigate robocalls, robocallers have less opportunity to originate scam calls on these networks. Instead, problematic robocalls increasingly are originating from VoIP numbers or toll-free numbers. TNS data show, for example, that VoIP continues to be the largest source of all unwanted calls – which TNS defines to include both nuisance calls and high-risk calls – at 53% of calls by volume, with toll-free numbers being used for 21% of calls.[5]

Under current law, only large voice service providers with more than 100,000 subscriber lines were required to implement STIR/SHAKEN in their IP networks by June 30, 2021. Although many smaller providers have at least partially implemented STIR/SHAKEN by

---

3 3rd FNPRM at ¶ 9.

4 Transaction Network Services Inc., TNS 2021 Robocall Investigation Report at 12 (2021), https://tnsi.com/forms/tns-2021-robocall-report/. (TNS 2021 Robocall Report).

5 *Id.* at 11. TNS uses analytics to classify calls into reputational categories reflecting the severity of the harm caused by the call behavior. "Nuisance" calls do not reflect malicious intent or intentional evasion of call restrictions, and involve moderate harm. Examples of nuisance calls are promotional offers, solicitation, and accounts receivables calls; *Id.* at 8. "High risk" calls reflect a knowing or willing transmission of misleading call identification information and/or a reckless disregard of legal standards. High risk calls typically cause emotional distress and severe harm, such as loss of money, invasion of privacy or identity theft; *Id.*

June 30, they are not required to fully implement STIR/SHAKEN for another two years.[6] TNS agrees with the Commission's proposal to curtail this extension for small voice service providers that originate an especially large amount of traffic.[7] With larger carriers generally having implemented call authentication technology, now is the time to look for the source of the remaining unwanted calls. Targeted, specific mandates can extend the progress that the industry has made in addressing unwanted robocalls while remaining faithful to the cost and implementation concerns the Commission expressed in the *Second Report and Order* in this docket.[8]

In the *Second Report and Order*, the Commission granted an extension to small voice providers "to allow small providers sufficient time to address challenges such as equipment cost and availability."[9] This blanket extension, however, applies regardless of the impact that a small provider's calls may have on the network and the harm that scam robocalls originating on small provider networks may cause consumers. This creates an opportunity for bad actors to continue their tactics by exploiting the networks of providers that have not fully implemented STIR/SHAKEN. Bad actors may continue to hide in networks with robocall mitigation protections that are not as robust as STIR/SHAKEN can provide. Moreover, bad actors that have been thwarted by large carrier implementation of STIR/SHAKEN will now be

---

6 *See STIR/SHAKEN Broadly Implemented Starting Today*, Press Release, DOC-373714A1 (rel. June 30, 2021) ("Over 200 voice service providers have certified to full STIR/SHAKEN implementation and hundreds more have certified to partial implementation—generally certifying to full implementation on the IP portions of their networks.").

7 3rd FNPRM at ¶ 1.

8 *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859 (2020).

9 *Id.* at ¶ 43.

seeking alternatives where the framework has not been implemented. For these reasons, it is appropriate for the Commission to shift its focus from a blanket extension to a more targeted rule that identifies the most common sources of unwanted robocalls and migrates those networks to STIR/SHAKEN as soon as possible.

A targeted approach provides significant public benefits. Primarily, the approach will benefit recipients of calls originated on these networks. These are the consumers who receive high risk calls and face the threat of a loss of money, invasion of privacy or identity theft from scam robocalls. Consumers lost more than $3.3 billion to fraud – an increase of nearly $1.5 billion over 2019.[10] High risk robocalls are more likely than other calls to be used to perpetrate such frauds, and the reduction in such calls will reduce the risk of harm that the public at large faces.[11] In the *First Report and Order* in this docket, the Commission estimated the benefit of reducing the nuisance from unwanted calls at $3 billion annually.

Further, as the Commission found in the *First Report and Order* in this proceeding, deployment of STIR/SHAKEN will reduce the nuisance consumers experience from unwanted calls, will restore confidence in Caller ID information, reduce disruptions to emergency and healthcare communications and reduce costs to voice service providers that must complete the unwanted calls.[12] These benefits will be more fully realized by requiring voice

---

10 *Consumer Sentinel Network Data Book 2020*, FEDERAL TRADE COMMISSION (Feb. 2020) *https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020.*

11 *See Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3263 ¶ 48 (2020) (implementation of STIR/SHAKEN "will significantly reduce the effectiveness of spoofing fraud that costs Americans billions of dollars each year, and similarly reduce the incidence of such fraud.") ("First Report and Order").

12 *Id.* at 3263-65, ¶¶ 47-51.

service providers that are more likely to be originating unwanted robocalls to implement STIR/SHAKEN more quickly.

These benefits are outweighed by any costs imposed on affected small providers. Most importantly, the cost of implementation of STIR/SHAKEN is reasonable. Small voice providers have several accessible solutions such as Call Guardian Authentication Hub from which they can choose. Call Guardian Authentication Hub offers a fully managed hosted solution that does not require the purchase of expensive equipment and reduces capital costs to small voice providers. Many small wireless providers, regional carriers and cable providers have successfully deployed this solution.[13] The widespread availability of such solutions is demonstrated by filings in the Robocall Mitigation Database, where the FCC acknowledged that over 200 voice service providers have certified to full implementation of STIR/SHAKEN with hundreds more certifying to partial implementation.[14] Indeed, as of July 7, 356 providers have certified to full implementation and 754 have certified to partial implementation of STIR/SHAKEN. If over 1,000 providers can implement STIR/SHAKEN at least in part, readily available, reasonable solutions are feasible for small voice providers at the greatest risk for generating high volumes of unwanted robocall traffic.

---

13 *See, e.g.*, CHARITON VALLEY, CV NEWS (2021), https://www.cvalley.net/call-guardian-service-provided-by-tns/; *Shenandoah Telecommunications Selects TNS Call Guardian for Robocall Detection*, TRANSACTION NETWORK SERVICES (April 13, 2021), https://tnsi.com/shenandoah-telecommunications-selects-tns-call-guardian-for-robocall-detection/; *Buckeye Broadband Taps TNS Call Guardian in Battle Against Robocalls*, TRANSACTION NETWORK SERVICES (July 30, 2020), https://tnsi.com/buckeye-broadband-taps-tns-call-guardian-in-battle-against-robocalls/; *Viaero Wireless Selects TNS Call Guardian for Robocall Protection*, TRANSACTION NETWORK SERVICES (May 12, 2020), https://tnsi.com/viaero-wireless-selects-tns-call-guardian-for-robocall-protection/; *Inland Cellular Deploys TNS Call Guardian to Protect Subscribers from Robocalls*, TRANSACTION NETWORK SERVICES (Sept. 4, 2019), https://tnsi.com/inland-cellular-deploys-tns-call-guardian-to-protect-subscribers-from-robocalls/.

14 *See supra,* fn 6.

In the *3rd FNPRM*, the Commission proposes several ways to identify those providers at the greatest risk for generating unwanted traffic. In the remainder of these comments, TNS offers its views on the effectiveness of the Commission's proposed solutions.

II. A NUMERICAL THRESHOLD FOR REQUIRING FASTER IMPLEMENTATION CAN BE EASILY EVADED

The Commission first seeks to define the affected service providers using a numerical threshold indicating an "unusually high number of calls per day on a single line."[15] While TNS applauds the Commission for focusing on those providers disproportionately originating calls, numerical thresholds are often ineffective at controlling robocalling behavior. First, there are legitimate reasons that a small voice service provider may originate a high volume of calls, particularly if the service provider specializes in serving enterprise customers. Thus, a pure numerical threshold may require implementation of STIR/SHAKEN by providers for whom the risk of unwanted calls is low. More importantly, the bad actors are adept at evading simple numerical thresholds. For example, TNS has long observed "snowshoe spamming" by robocallers. Snowshoe spamming is robocalling behavior that seeks to evade blocking thresholds by spreading their activity over a large number of telephone numbers, so that the volume on any single number does not exceed the detection thresholds.[16] TNS has observed an increase in bad actors that are using low-volume spamming across a large amount of telephone numbers while attempting to avoid analytics engines. The two most common

---

15 3rd FNPRM at ¶ 21. The Commission also seeks comment on a revenue threshold for identifying affected service providers; *Id.* at ¶ 26. TNS' analytics data does not use service provider revenue as an input, and it is unaware of relevant, reliable data that would identify such providers. Moreover, nothing in TNS' analytics data suggests that problematic robocalls are correlated with the provision of non-mass market services.

16 TNS 2021 Robocall Report at 7.

techniques involve either mimicking call patterns of a small to medium sized business and spreading calls over a large number of telephone numbers leased from VoIP wholesalers, or spreading a very low volume of calls across a very large set of telephone numbers via spoofing. Typically, the telephone numbers used will come from a number that is from the same area code or local calling area to incent the subscriber to pick up. Thus, a numerical threshold is unlikely to be effective at identifying the service providers most at risk of originating unwanted calls.

III. THE COMMISSION SHOULD TARGET ITS RULE TO ALL-IP VOIP PROVIDERS AND SMALL VOIP PROVIDERS THAT OFFER SERVICES THAT ENCOURAGE OR ENABLE ROBOCALLING

The Commission also asks whether alternative or additional criteria would better target the source of illegal robocalls. TNS agrees with two of the alternatives suggested.

First, as USTelecom has noted, many smaller companies that provide IP-based voice service are responsible for originating disproportionate numbers of illegal robocalls.[17] TNS data bears this out. VoIP telephone numbers accounted for 54% of high risk calls in 2020, according to TNS' data.[18] One of the primary reasons for this is that VoIP networks make it relatively easy to spoof telephone numbers. Service providers that are exclusively VoIP can quickly become the networks of choice for bad actors looking to evade STIR/SHAKEN implementations from larger service providers. The Commission therefore should consider using whether a service provider is all-VoIP as at least one criterion for identifying the service providers subject to an accelerated deadline.

---

17 Letter from Joshua M. Bercu, Vice President, Policy & Advocacy, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 5-6 (filed Sept. 18, 2020).

18 TNS 2021 Robocall Report at 11.

Second, the Commission should look closely at service providers that offer or enable spoofing services. In TNS' experience, a provider that allows users to bring their own call origination platforms or that unbundles service so that direct inbound numbers may be purchased separately from outbound calling minutes are correlated to problematic calls. By contrast, a carrier that uses proprietary hardware standards or prevents user hardware from altering carrier configuration settings is less likely to results in spoofing of telephone numbers. TNS recommends that the Commission explore ways to identify these service providers and to shorten its implementation deadlines for those providers that employ such techniques.

IV. THE COMMISSION SHOULD ALSO EMPOWER THE ENFORCEMENT BUREAU TO DIRECT IMPLEMENTATION OF STIR/SHAKEN IN ITS CEASE-AND-DESIST LETTERS

In addition to creating a general rule for certain providers, the Commission should also empower the Enforcement Bureau to direct implementation in response to demonstrated issues involving problematic robocalls. The Commission has already empowered the Enforcement Bureau to notify an originating or intermediate provider when it has failed to effectively mitigate illegal traffic and to require such providers to take action to mitigate such calls within 48 hours.[19] TNS recommends that the Commission strengthen this procedure by empowering the Bureau to direct the originating or intermediate provider to implement STIR/SHAKEN as a remedy to the deficiency in mitigating illegal traffic. Specifically, TNS recommends that, in addition to directing the provider to mitigate the identified traffic within 48

---

[19] 47 C.F.R. § 64.1200(k)(4); The Enforcement Bureau has used this authority on several occasions already. *See, e.g.,* Letter to VaultTel Solutions, DOC-372308A1, (May 18, 2021).

hours, the Bureau be empowered to direct the provider to either (a) implement STIR/SHAKEN within 30 days or (b) submit a modified Robocall Mitigation Plan for Bureau approval.

This proposal allows the Bureau to direct faster implementation of STIR/SHAKEN for those providers with a demonstrated record of originating or transiting illegal robocall traffic. This measure would provide the Commission with the tools to target the most significant sources of illegal traffic and to protect the public from harm from such traffic. Thirty days should be sufficient time to implement STIR/SHAKEN, given marketplace alternatives available and the now extensive industry experience in deploying STIR/SHAKEN solutions. If it is not sufficient time, however, the provider can instead submit a revised Robocall Mitigation Plan, which would be reviewed and approved by the Bureau. Thus, any provider that claims an inability to implement STIR/SHAKEN would have an alternative means of mitigating illegal traffic on its network.

V. CONCLUSION

For the foregoing reasons, TNS supports the Commission's efforts to promote the development of advanced methods to combat unlawful robocalls. Through a combination of robust analytics inputs and greater trust and authentication in the telecommunications network, TNS believes that the industry can make a material impact on the problem.

Respectfully submitted,

Lavinia Kennedy
James Tyrrell
Paul Florack
TRANSACTION NETWORK SERVICES, INC.
10740 Parkridge Blvd.
Suite 100
Reston, VA 20191
(703) 453-8300
lkennedy@tnsi.com
jtyrrell@tnsi.com
pflorack@tnsi.com

Steven A. Augustino
Belen Crisp*
KELLEY DRYE & WARREN LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
(202) 342-8612
saugustino@kelleydrye.com

Its Counsel

* Ms. Crisp is admitted only in Maryland and is supervised by principals of the firm who are members of the DC Bar.

July 9, 2020